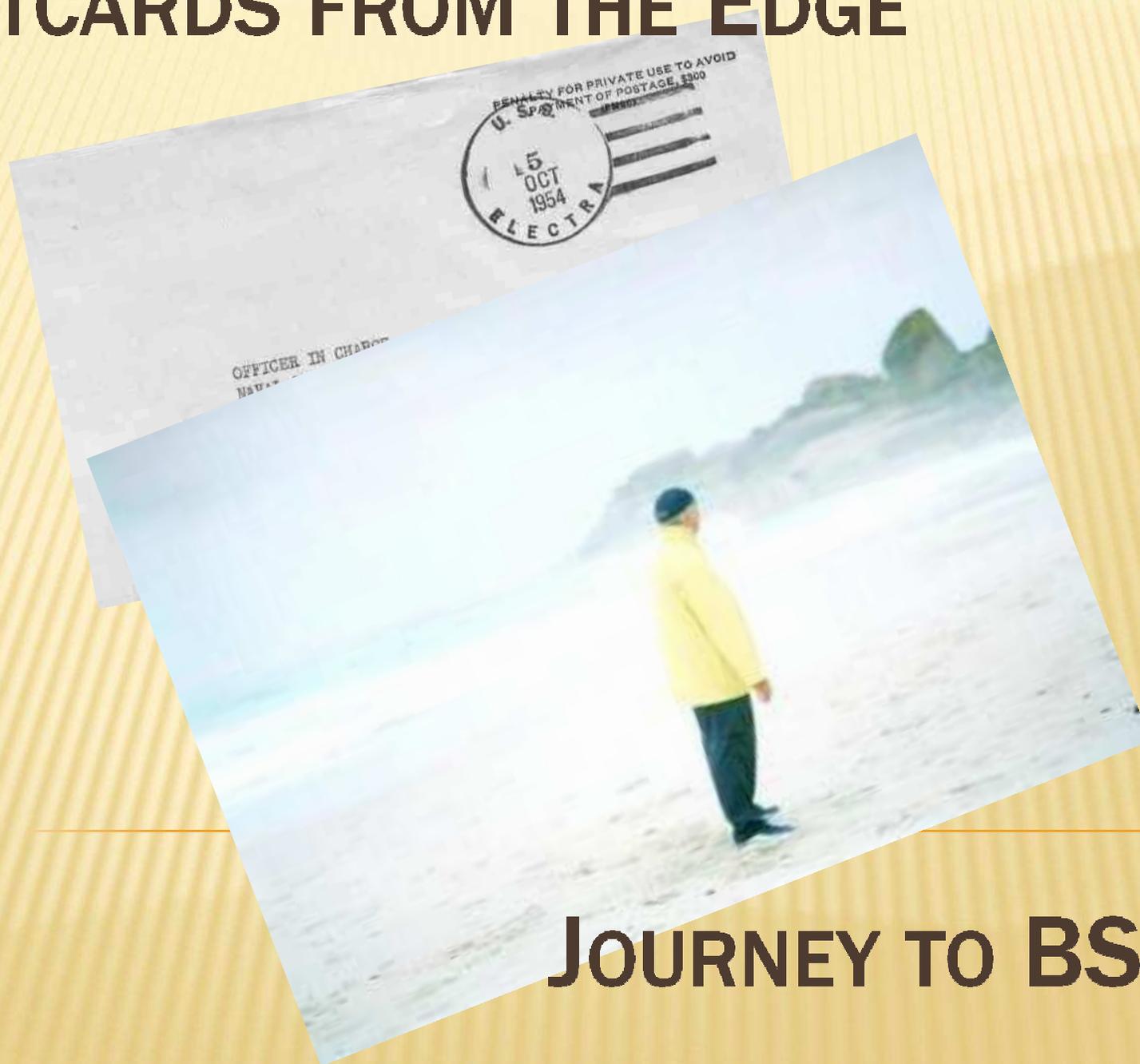


# POSTCARDS FROM THE EDGE

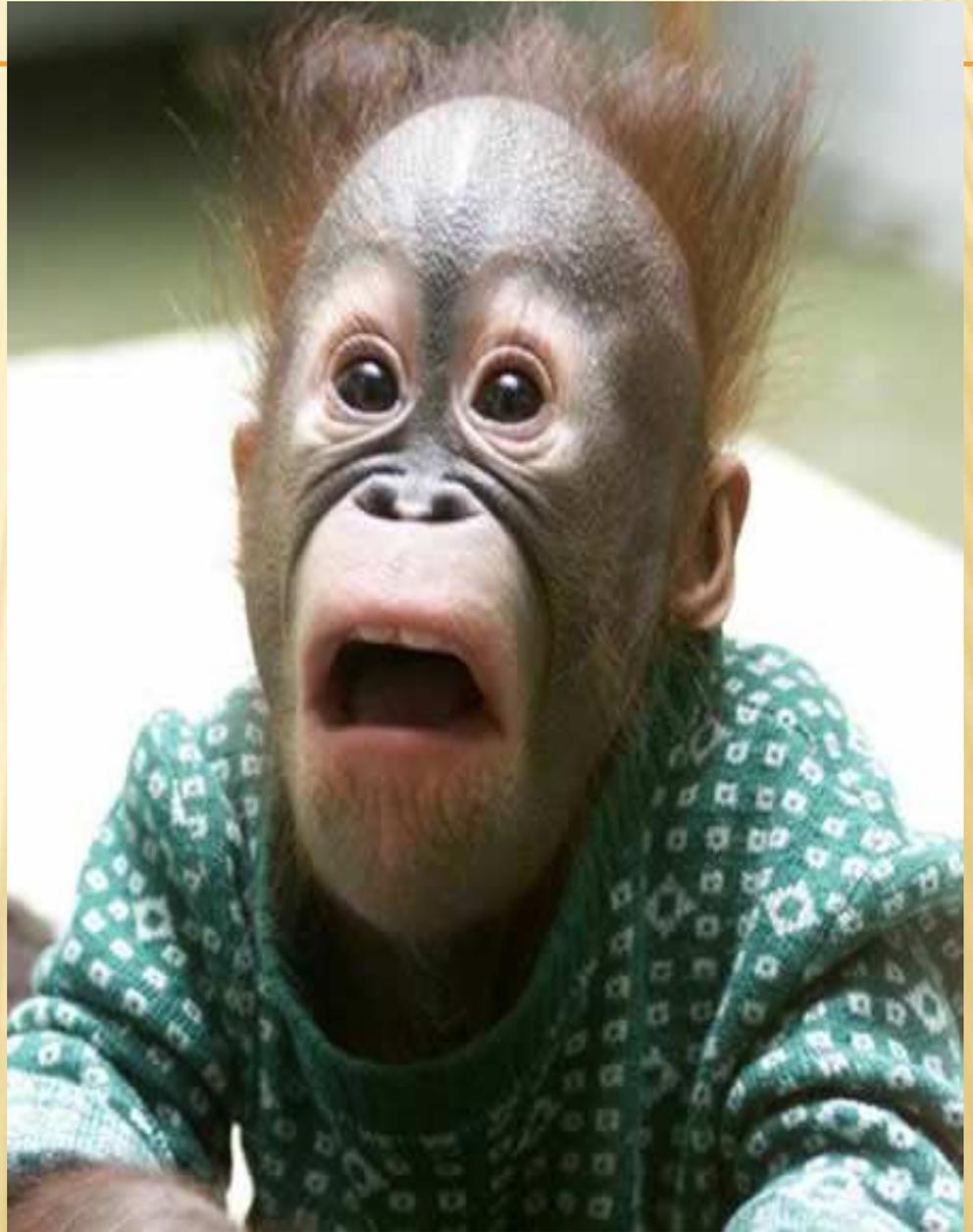


**JOURNEY TO BSIMM**

# CLINICAL TRIAL RESULTS

---

**BEFORE BSIMM**



**AFTER 3 MONTHS ON  
BSIMM**



# MY TOP FOUR SECURITY ISSUES

---

1. Communications
2. Compliance
3. Technology
4. Bad Guys

# BSIMM IN 4 DOMAINS:

## THE SOFTWARE SECURITY FRAMEWORK (SSF)

---

1. **Governance:** Practices that help organize, manage, and measure a software security initiative. Staff development is also a central governance practice.
2. **Intelligence:** Practices that result in collections of corporate knowledge used in carrying out software security activities throughout the organization. Collections include both proactive security guidance and organizational threat modeling.
3. **SDL Touchpoints:** Practices associated with analysis and assurance of particular software development artifacts and processes. All software security methodologies include these practices.
4. **Deployment:** Practices that interface with traditional network security and software maintenance organizations. Software configuration, maintenance, and other environment issues have direct impact on software security.

# TACKLING COMMUNICATIONS – BSIMM

---

- ✘ It is what we do – NOT what we should do
- ✘ Represents “true” picture of best practice.
- ✘ A mechanism to propel effective communications
- ✘ Quantitative
- ✘ 110 tasks in 12 practices in 4 domains – ability to “click up” or “drill down”
- ✘ Builds confidence in security across the enterprise

# THE EPIPHANY – A CASE STUDY IN CLICK-UP COMMUNICATIONS

---

- ✘ Need: Effective CEO Communications
  - + Resource commitment
  - + Top-down support
  - + Getting “a seat at the table”
  
- ✘ CEO’s really tough question: “How do we know if we are feeding our baby enough?”
- ✘ CISO’s really bad answer: “Trust me!”
- ✘ Result: Bad karma
- ✘ Leveraging BSIMM to change the outcome
  - + Focus on end-state relative to our peers
  - + Ability to show a competitive discriminator
  - + Provide a basis for objective discussion on processes and ways to shore-up weaknesses

# THE FIX IS IN: A CASE STUDY IN DRILL-DOWN FOR IT

- ✘ Need: An effective mechanism to influence IT architecture and SDLC
  - + Effective and efficient security architecture and the SDLC review & testing
  - + Develop long-term thinking
  - + Develop security as thought leader and “owning the outcome”
  - + Measurable results
- ✘ Architecture and development: Committed to delivering feature and function on limited resources
- ✘ CISO: Committed to ensuring security of all applications
- ✘ Leveraging BISMM to eliminate tension
  - + Demonstrate our peer group’s efforts
  - + Define best practice
  - + Provide the foundation for a IT security roadmap

# IN THE END

---

You've got to be very careful if you don't know where you're going, because you might not get there.”

*Yogi Berra 1925*